WHAT IS CLAIMED IS:

1. A digital signature generating apparatus having storage unit in which a plurality of secret keys have been stored, comprising:

a processing unit adapted to change a secret key used by said digital signature generating apparatus to a secret key specified by a key change command if the key change command has been received, and generate a digital signature of prescribed digital data using any one of the plurality of secret keys if a signature generating command has been received.

2. The apparatus according to claim 1, wherein said apparatus is an IC card.

3. The apparatus according to claim 2, wherein said apparatus is an apparatus equipped with a multi-application operating system.

4. The apparatus according to claim 1, wherein the key change command is a command that includes information specifying any one of the plurality of secret keys.

5. The apparatus according to claim 1, wherein the signature generating command is a command that includes the prescribed digital data or hash thereof.

6. A method of generating a digital signature in a digital signal generating apparatus having storage unit in which a plurality of secret keys have been stored, said method comprising the steps of:

changing a secret key used by said digital signature generating apparatus to a secret key specified by a key change command if the key change command has been received; and

generating a digital signature of prescribed digital data using any one of the plurality of secret keys if a signature generating command has been received.

7. The method according to claim 6, wherein said apparatus is an IC card.

8. The method according to claim 7, wherein said apparatus is an apparatus equipped with a multi-application operating system.

9. The method according to claim 6, wherein the key change command is a command that includes information specifying any one of the plurality of secret keys.

10. The method according to claim 6, wherein the signature generating command is a command that includes the prescribed digital data or hash thereof.

11. A computer program for causing a computer to execute each of the steps of the method of generating a digital signature set forth in claim 6.

12. A computer-readable storage medium on which the computer program set forth in claim 11 has been stored.

13. A digital signature generating apparatus, which has a plurality of secret keys, for generating a digital signature of prescribed digital data using one

of the plurality of secret keys, comprising:

a processing unit adapted to analyze an externally applied command, and set a secret key, which is to be used in generating the digital signature, from among the plurality of secret keys in accordance with result of the analysis.